RECEIVED
CENTRAL FAX CENTER
JAN 0 9 2008

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method comprising:

initializing a pseudo-random number generator (PRNG);

obtaining local seeding information from a host;

securely obtaining remote seeding information from remote entropy servers via a secure entropy collection protocol, the secure entropy protocol relying on unpredictable random numbers ~~and providing interaction between the remote entropy servers~~, each of the remote entropy servers having a random state machine generating the remote seeding information, the remote seeding information to be mixed with the local seeding information ~~to cause continuous randomness~~ to provide an unpredictable system status to amplify entropy to enhance system security, wherein the remote seeding information is to facilitate unpredictability of the unpredictable system status, wherein the enhancing of the system security includes securing an initial seed state via the remote entropy servers;

repeating the securely obtaining of the remote seeding information for each entropy server;

generating a key pair including a temporary asymmetric public key and a temporary asymmetric private key;

encrypting the temporary public key with a public key associated with a remote entropy server;

decrypting the temporary public key with a private key associated with the remote entropy server;

encrypting the remote seeding information with the temporary public key;

decrypting the remote seeding information with the temporary private key; and

stirring the PRNG via the local seeding information and the remote seeding information.

2. (Previously Presented) The method of claim 1, wherein the initializing of the PRNG comprises initializing an internal state of the PRNG with a random value.

3. (Previously Presented) The method of claim 2, wherein the random value comprises a seed.

4. (Cancelled)

5. (Previously Presented) The method of claim 1, wherein the remote entropy servers maintain random state pool to supply the host with the random value.

6. (Previously Presented) The method of claim 1, wherein the obtaining of the remote seeding information from the remote entropy servers is performed via a privacy protocol.

7. (Original) The method of claim 6, wherein the privacy protocol comprises secure sockets layer (SSL) protocol.

8. (Original) The method of claim 6, wherein the privacy protocol comprises transport layer security (TLS) protocol.

9. (Previously Presented) The method of claim 1, wherein the stirring of the PRNG comprises producing a cryptographically random stream of bits.

Claims 10-16 (Cancelled)

17. (Currently Amended) An entropy enhancing system comprising:

a host at a local computer system coupled with remote entropy servers at remote computer systems; and

a server computer system coupled with the local computer system and the remote computer systems, the server to

initialize a pseudo-random number generator (PRNG) by obtaining local seeding information from the host,

securely obtain remote seeding information from the remote entropy servers via a secure entropy collection protocol, the secure entropy protocol relying on unpredictable random numbers ~~and providing interaction between the remote entropy servers~~, each of the remote entropy servers having a random state machine generating the remote seeding information, the remote seeding information to be mixed with the local seeding information ~~to cause continuous randomness~~ to provide an unpredictable system status to amplify entropy to enhance system security, wherein the remote seeding information is to facilitate unpredictability of the unpredictable system status, wherein the enhancing of the system security includes securing an initial seed state via the remote entropy servers,

repeating the securely obtaining of the remote seeding information for each entropy server,

generate a key pair including a temporary asymmetric public key and a temporary asymmetric private key,

encrypt the temporary public key with a public key associated with a remote entropy server,

decrypt the temporary public key with a private key associated with the remote entropy server

encrypt the remote seeding information with the temporary public key,

decrypt the remote seeding information with the temporary private key, and

stir the PRNG via the local seeding information and the remote seeding information.

18. (Previously Presented) The entropy enhancing system of claim 17, wherein the local computer system to generate the local seeding information via the host.

19. (Previously Presented) The entropy enhancing system of claim 17, wherein the remote computer systems are to generate the remote seeding information via the remote entropy servers.

Claims 20-24 (Cancelled)

25. (Currently Amended) A machine-readable medium having instructions which, when executed, cause a machine to:

initialize a pseudo-random number generator (PRNG);

obtain local seeding information from a host;

securely obtain remote seeding information from remote entropy servers via a secure entropy collection protocol, the secure entropy protocol relying on unpredictable random numbers ~~and providing interaction between the remote entropy servers~~, each of the remote entropy servers having a random state machine generating the remote seeding information, the remote seeding information to be mixed with the local seeding information ~~to cause continuous randomness~~ to provide an unpredictable system status to amplify entropy to enhance system security, wherein the remote seeding information is to facilitate unpredictability of the unpredictable system status, wherein the enhancing of the system security includes securing an initial seed state via the remote entropy servers;

repeat the securely obtaining of the remote seeding information for each entropy server;

generate a key pair including a temporary asymmetric public key and a temporary asymmetric private key;

encrypt the temporary public key with a public key associated with a remote entropy server;

decrypt the temporary public key with a private key associated with the remote entropy server;

encrypt the remote seeding information with the temporary public key;

decrypt the remote seeding information with the temporary private key; and

stir the PRNG via the local seeding information and the remote seeding information.

26. (Previously Presented) The machine-readable medium of claim 25, wherein the instructions when executed to initialize the PRNG further cause the machine to initialize an internal state of the PRNG with a random value.

27. (Previously Presented) The machine-readable medium of claim 26, wherein the random value comprises a seed.

28. (Cancelled)

29. (Previously Presented) The machine-readable medium of claim 25, wherein the instructions when executed, further cause the machine to maintain random state pool to supply the host with the random value.

30. (Previously Presented) The machine-readable medium of claim 25, wherein the instructions when executed to stir the PRNG further cause the machine to produce a cryptographically random stream of bits.